PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-220686

(43)Date of publication of application : 10.08.1999

(51)Int.Cl. H04N 5/765
H04N 5/781
G09C 1/00
H04L 9/32
H04N 5/225
H04N 5/232
H04N 5/915

(21)Application number : 10-035421

(22)Date of filing : 02.02.1998

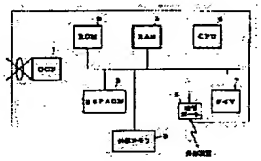
(71)Applicant : RICOH CO LTD

(72)Inventor : KANAI YOICHI
YANAIDA MASUYOSHI
NUMAZAWA MIEKO

(54) DIGITAL CAMERA

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a digital camera in which the proving strength of photographed picture data can be improved.



SOLUTION: When a shutter button is pressed, a CPU 4 obtains a time from a timer, and stores it in an RAM 3, and obtains photographic picture data from a CCD 1, and houses the data in the RAM 3, and compresses the housed picture data. Also, the CPU 4 extracts a sequence number from an EEPROM 5, and records a sequence number obtained by adding 1 to the sequence number in the EEPROM 5. The sequence number and the time data are added to the leading of the compressed picture data. A message digest using a message digest algorithm is calculated for the prepared picture information. A secret key is read from the EEPROM 5, and the message digest is enciphered. The obtained signature is added to the tail of the previous picture information so that a group of photographic information can be obtained, and recorded in an outside memory 8.

LEGAL STATUS

[Date of request for examination] 09.06.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]
[Claim 1] The digital camera characterized by having held as the public key certificate which consists of a digital signature of the authentication [as opposed to / at least / a public key and this public key for the public key and private key of a pair] engine used for authentication of a public key cryptosystem, and a private key, and carrying the cryptographic algorithm of a public key cryptosystem, and the generation algorithm of a message digest.
[Claim 2] The digital camera characterized by enciphering inside using said private key and recording the message digest calculated inside from the image data to which said held private key had and photoed the external read-out inhibited attribute in the digital camera according to claim 1 on a storage with said image data.
[Claim 3] The digital camera with which said held public key certificate is characterized by having a rewriting inhibited attribute from the outside in claim 1 or a digital camera given in 2.
[Claim 4] The digital camera characterized by rewriting of said held private key or a public key certificate being possible when the external authentication key of at least 1 is held and the external authentication over this external authentication key is materialized in a digital camera according to claim 1 to 3.
[Claim 5] The digital camera characterized by what is recorded on a storage with the image data which held the sequence number which expresses the number of sheets of the photoed image in a digital camera according to claim 1 to 4, and photoed this sequence number.
[Claim 6] The digital camera with which said held sequence number is characterized by having a rewriting inhibited attribute from the outside in a digital camera according to claim 5.
[Claim 7] The digital camera characterized by enciphering inside using said held private key, and recording on a storage the message digest calculated inside from the image information which combined said sequence number and said image data with claim 5 or 6 in the digital camera of a publication with said image information.
[Claim 8] The digital camera characterized by reset of said held sequence number being possible when the external authentication key of at least 1 is held and the external authentication over this external authentication key is materialized in a digital camera according to claim 5 to 7.
[Claim 9] The digital camera characterized by enciphering inside using said held private key, and recording on a storage the message digest calculated inside from the image information which combined the time of day which photoed image data, and this image data in the digital camera according to claim 1 to 8 with said image information.
[Claim 10] The digital camera with which a setup of the time of day managed inside is characterized by having a modification inhibited attribute from the outside in a digital camera according to claim 9.
[Claim 11] The digital camera characterized by setting modification of the time of day managed inside when the external authentication key of at least 1 is held and this external authentication key is materialized being possible in claim 9 or a digital camera given in 10.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to a security system applicable to general data security about the security of a digital camera and the image data photoed with the digital camera in the detail more.
[0002]
[Description of the Prior Art] As a technique which photos an image of evidence with a digital camera, JP,7-50827,A "the accident monitoring system using a digital electronic camera" is mentioned, for example. This raises the proof nature of image data by recording the image related information of an accident related situation correctly to the image data photoed about the accident monitoring system using the digital camera carried in an automobile, and forbidding rewriting of **** of evidence or data further. In the claim 2, there is a publication "it is characterized by enabling elimination and writing by the code setting approach of fixed conditions", and the part becomes a technique used as the nucleus which prevents destruction of evidence and an alteration of image data.
[0003]
[Problem(s) to be Solved by the Invention] However, it cannot carry out by there being no indication of the concrete technique about the above-mentioned code setup or an approach in the example of above-mentioned JP,7-50827,A. Moreover, it is very difficult conventionally for a coma in a film to be serially located in a line, and for the photograph taken using the usual film to understand the order relation of the fact photoed when referring to the developed film from the photoed sequence being clear, and to forge the film moreover, to replace the photoed sequence or to change an image. However, the image data photoed with the digital camera is easy to perform an alteration, elimination, exchange of data, etc., without leaving no trace, since the data itself are digital, and the present condition is that the photoed image, i.e., the factual certification force, is low compared with what was photoed with the camera of the conventional film base.
[0004] This invention was made in consideration of the above actual condition, and is made for the purpose of offering the digital camera which heightened the certification force of the photoed image data.
[0005]
[Means for Solving the Problem] Invention of claim 1 is held as the public key certificate which consists of a digital signature of the authentication [as opposed to / at least / a public key and this public key for the public key and private key of a pair] engine used for authentication of a public key cryptosystem, and a private key, is characterized by carrying the cryptographic algorithm of a public key cryptosystem, and the generation algorithm of a message digest, is a digital camera simple substance and adds a signature to image data.
[0006] In invention of claim 1, invention of claim 2 is characterized by enciphering inside using said private key and recording the message digest calculated inside from the image data to which said held private key had and photoed the external read-out inhibited attribute on a storage with said image data, and raises the security of a signature.

[0007] Said held public key certificate is characterized by having a rewriting inhibited attribute from the outside, and invention of claim 3 enables it to ensure verification of the signature added to image data in claim 1 or invention of 2.
[0008] Invention of claim 4 enables it to change the private key and public key certificate which are held in invention of claim 1 thru/or invention of three either, only when it is characterized by rewriting of said held private key or a public key certificate being possible when the external authentication key of at least 1 is held and the external authentication over this external authentication key is materialized and special conditions are fulfilled.
[0009] In invention of claim 1 thru/or either of 4, invention of claim 5 holds the sequence number showing the number of sheets of the photoed image, is characterized by what is recorded on a storage with the image data which photoed this sequence number, and records the sequence number of an image.
[0010] Said held sequence number is characterized by having a rewriting inhibited attribute from the outside, and invention of claim 6 prevents from changing the sequence number of an image from the outside in invention of claim 5.
[0011] Invention of claim 7 is characterized by enciphering inside using said held private key, and recording on a storage the message digest calculated inside from the image information which combined said sequence number and said image data with said image information, and prevents from separating a sequence number and image data in claim 5 or invention of 6.
[0012] in invention of claim 5 thru/or either of 7, invention of claim 8 could reset [having made and] the sequence number held, only when it was characterized by reset of said held sequence number being possible when the external authentication key of at least 1 is held and the external authentication over this external authentication key is materialized and special conditions were fulfilled.
[0013] Invention of claim 9 is characterized by enciphering inside using said held private key, and recording on a storage the message digest calculated inside from the image information which combined the time of day which photoed image data, and this image data in invention of claim 1 thru/or either of 8 with said image information, and records a setup of the time of day managed inside in the condition that it is unseparable with image data.
[0014] A setup of the time of day managed inside is characterized by having a modification inhibited attribute from the outside, and invention of claim 10 prevents from changing from the outside a setup of the time of day managed inside in invention of claim 9.
[0015] Invention of claim 11 enables it to change a setup of the time of day managed inside in claim 9 or invention of 10, only when it is characterized by setting modification of the time of day managed inside when the external authentication key of at least 1 is held and this external authentication key is materialized being possible and special conditions are fulfilled.
[0016]
[Embodiment of the Invention] a block diagram for drawing 1 to explain one example of the digital camera by this invention -- it is -- the inside of drawing, and 1 -- CCD and 2 -- ROM and 3 -- RAM and 4 -- CPU and 5 -- EEPROM and 6 -- a communication link port and 7 -- a timer and 8 -- external memory -- it is -- cryptographic algorithm (for example, RSA and DES (Data Encryption Standard) which are shown in a U.S. Pat. No. 4405829 number.) standard to ROM2 DES may be used for external authentication. A message digest generation algorithm (for example, MD5), an image data compression algorithm (for example, JPEG), a random-number-generation algorithm, and the Maine control program are stored. The private key of a public key cryptosystem, and a public key certificate (an authentication engine's signature and public key), a sequence number and an external authentication key are stored in EEPROM5. The Maine control program, various algorithms, a private key, a sequence number, an external authentication key, etc. are loaded to RAM3 if needed. The image information which added a sequence number, time of day, a signature, etc. to the photoed image data is recorded on external memory (for example, memory card etc.) 8. In addition, an algorithm means a program here.

[0017] If a shutter release is pushed, CPU4 will acquire photography image data from CCD1, and will hold it in RAM3 at the same time it acquires time of day from a timer and memorizes it to RAM3. And the held image data is compressed. The sequence number added to the sequence number one is recorded on EEPROM5 at the same time it takes out a sequence number from EEPROM5. Next, the sequence number previously taken out at the head of the compressed image data and the time-of-day data acquired from the timer are added. And the message digest which used the message digest algorithm (for example, MD5) to the done image information is calculated. A private key is read from EEPROM5 and the message digest previously calculated using it is enciphered. And the obtained signature is added to the last of previous image information, and it considers as the photography information on a lump, and records on external memory 8.
[0018] In case a private key, a public key certificate, a sequence number, and a time-of-day setup are changed, the following procedures perform external authentication processing which should be performed beforehand. When the algorithm used for external authentication is DES, first, a random number is generated inside and the random number is sent out to an external device. It compares with the code which enciphered the authorization code with reception from the external device, and enciphered the random number generated previously with the external authentication key. It supposes that external authentication was materialized when those codes were in agreement, and is the security status (flag managed by RAM.). An initial state is set to FALSE. It changes into TRUE.
[0019] With reference to the security status first managed inside when modification of a private key, a public key certificate, a sequence number, and a time-of-day setup is required from the exterior, when it serves as FALSE, a demand is not received. When it is TRUE, a demand is received, and processing according to the demand is performed. Processing changes the security status into FALSE.
[0020]
[Effect of the Invention] Use invention of claim 1 for authentication of a public key cryptosystem, and even if few, the public key and private key of a pair Since it held as the public key certificate which consists of an authentication engine's digital signature to a public key and this public key, and a private key and the cryptographic algorithm of a public key cryptosystem and the generation algorithm of a message digest were carried In case a signature is added to the photoed image, with required information and an algorithm, a signature can be added to image data with a digital camera simple substance, and the certification force of the photoed image data can be heightened.
[0021] Invention of claim 2 is set to invention of claim 1. Said held private key Since it enciphers inside using said private key and the message digest which has an external read-out inhibited attribute and calculated it inside from the photoed image data is recorded on a storage with said image data The reference from the outside of the private key used for generation of a signature becomes impossible. By this By being able to raise the security of a signature and adding a signature (what enciphered the message digest) to the image data which photoed the signature (what enciphered the message digest) in the photoed image The digital camera which photoed image data can be specified and the certification force of the photoed image data can be heightened.
[0022] In claim 1 or invention of 2, since said held public key certificate has a rewriting inhibited attribute from the outside, rewriting of it from the outside of a public key certificate becomes impossible, invention of claim 3 can ensure by this verification of the signature added to image data with the digital camera, can specify the digital camera which photoed image data, and can heighten the certification force of the photoed image data.
[0023] When invention of claim 4 holds the external authentication key of at least 1 in invention of claim 1 thru/or either of 3 and the external authentication over this external authentication key is materialized Since rewriting of said held private key or a public key certificate is possible Only when special conditions are fulfilled, modification of the private key held and a public key certificate is attained. By this The certification force of the image which could carry out things, renewal of a still more nearly periodical key was attained, and the security of a private key increased, and was photoed which

maintains the security of a private key or a public key certificate can be heightened.
[0024] In invention of claim 1 thru/or either of 4, invention of claim 5 holds the sequence number showing the number of sheets of the photoed image, and since it records on a storage with the image data which photoed this sequence number, it can heighten the certification force about the context of the fact realized with the camera of the film base by record of the sequence number of an image.
[0025] In invention of claim 5, since said held sequence number has a rewriting inhibited attribute from the outside, modification of invention of claim 6 from the outside of the sequence number of an image becomes impossible, and thereby, it can raise the security of a sequence number and can heighten the certification force about a factual context.
[0026] Invention of claim 7 the message digest calculated inside in claim 5 or invention of 6 from the image information which combined said sequence number and said image data Since it enciphers inside using said held private key and records on a storage with said image information A message digest can be calculated by the ability to double a sequence number and image data, a signature can be created, it can be made by this what cannot separate a sequence number and image data, and the sequence number can raise the certification force about a factual context.
[0027] Since reset of said held sequence number is possible for invention of claim 8 when the external authentication key of at least 1 is held and the external authentication over this external authentication key is materialized in invention of claim 5 thru/or either of 7 By making resettable the sequence number held, only when special conditions are fulfilled By being able to maintain the security of a sequence number and resetting a sequence number still more nearly periodically It can prevent being able to manage a sequence number in the range which is useful for proving a factual context, and a sequence number's becoming large recklessly, and becoming the number which is hard to treat.
[0028] Invention of claim 9 the message digest calculated inside from the image information which combined the time of day which photoed image data, and this image data in invention of claim 1 thru/or either of 8 Since it enciphers inside using said held private key and records on a storage with said image information, it can record in the condition that the time of day managed inside is unseparable with image data, and, thereby, the certification force about the time of day when image data was photoed can be heightened.
[0029] In invention of claim 9, a setup of the time of day managed inside enables modification from the outside of a time-of-day setup managed inside since it has a modification inhibited attribute from the outside, and can raise the security about a setup of time of day by this, and invention of claim 10 can heighten the certification force about the time of day when image data was photoed.
[0030] Since setting modification of the time of day managed inside when the external authentication key of at least 1 is held and this external authentication dark is materialized in claim 9 or invention of 10 is possible for invention of claim 11 Only when special conditions are fulfilled, modification of a time-of-day setup managed inside is enabled, thereby, maintaining the security about a setup of time of day, it can be periodically set as exact time of day, and the certification force about the time of day when image data was photoed can be heightened.

[Translation done.]

2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is a block diagram for explaining one example of the digital camera by this invention.
[Description of Notations]
1 [-- CPU, 5 / -- EEPROM, 6 / -- A communication link port, 7 / -- A timer, 8 / -- External memory.] -- CCD, 2 -- ROM, 3 -- RAM, 4

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－220686

(43)公開日　平成11年(1999)８月10日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｎ	5/765		Ｈ０４Ｎ	5/781	５１０Ｌ
	5/781		Ｇ０９Ｃ	1/00	６４０Ｂ
Ｇ０９Ｃ	1/00	６４０	Ｈ０４Ｎ	5/225	Ｚ
Ｈ０４Ｌ	9/32				Ｃ
Ｈ０４Ｎ	5/225			5/232	Ｚ

審査請求　未請求　請求項の数11　ＦＤ　（全５頁）　最終頁に続く

(21)出願番号　特願平10－35421

(22)出願日　平成10年(1998)２月２日

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号

(72)発明者　金井　洋一
東京都大田区中馬込１丁目３番６号　株式会社リコー内

(72)発明者　谷内田　益義
東京都大田区中馬込１丁目３番６号　株式会社リコー内

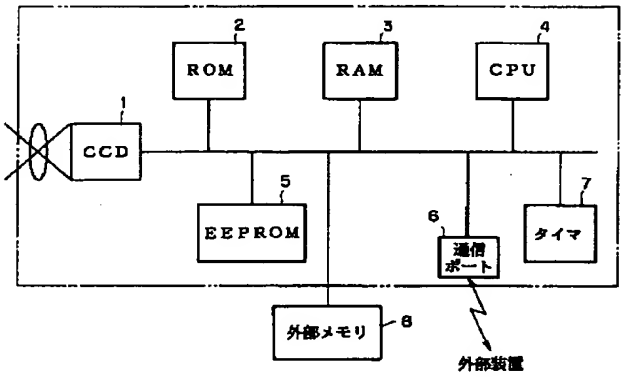
(72)発明者　沼沢　美恵子
東京都大田区中馬込１丁目３番６号　株式会社リコー内

(54)【発明の名称】　デジタルカメラ

(57)【要約】

【課題】　撮影した画像データの証明力を高めたデジタルカメラを提供する。

【解決手段】　シャッターボタンが押されると、ＣＰＵ４はタイマから時刻を取得し、それをＲＡＭ３に記憶すると同時に、ＣＣＤ１から撮影画像データを取得してＲＡＭ３に収容し、収容した画像データを圧縮する。ＥＥＰＲＯＭ５からシーケンス番号を取り出すと同時に、シーケンス番号に１加えたシーケンス番号をＥＥＰＲＯＭ５に記録する。圧縮した画像データの先頭にシーケンス番号と、時刻データとを付加する。できあがった画像情報に対してメッセージダイジェストアルゴリズムを使用したメッセージダイジェストを計算する。ＥＥＰＲＯＭ５から秘密鍵を読み出し、メッセージダイジェストを暗号化する。得られた署名を先の画像情報の最後に付加して一塊の撮影情報とし、外部メモリ８に記録する。



1

【特許請求の範囲】

【請求項１】　公開鍵暗号方式の認証に用いる少なくとも一対の公開鍵及び秘密鍵を、公開鍵と該公開鍵に対する公証機関のデジタル署名とからなる公開鍵証明書及び秘密鍵として収容し、公開鍵暗号方式の暗号アルゴリズムとメッセージダイジェストの生成アルゴリズムとを搭載したことを特徴とするデジタルカメラ。

【請求項２】　請求項１に記載のデジタルカメラにおいて、前記収容した秘密鍵が、外部読出禁止属性を有し、撮影した画像データから内部で計算したメッセージダイジェストを、前記秘密鍵を用いて内部で暗号化し、前記画像データとともに記憶媒体に記録することを特徴とするデジタルカメラ。

【請求項３】　請求項１あるいは２に記載のデジタルカメラにおいて、前記収容した公開鍵証明書が、外部からの書換禁止属性を有することを特徴とするデジタルカメラ。

【請求項４】　請求項１乃至３のいずれかに記載のデジタルカメラにおいて、少なくとも一の外部認証鍵を収容し、該外部認証鍵に対する外部認証が成立することにより、前記収容した秘密鍵あるいは公開鍵証明書の書き換えが可能であることを特徴とするデジタルカメラ。

【請求項５】　請求項１乃至４のいずれかに記載のデジタルカメラにおいて、撮影した画像の枚数を表わすシーケンス番号を収容し、該シーケンス番号を、撮影した画像データとともに記憶媒体に記録することを特徴とするデジタルカメラ。

【請求項６】　請求項５に記載のデジタルカメラにおいて、前記収容したシーケンス番号が、外部からの書換禁止属性を有することを特徴とするデジタルカメラ。

【請求項７】　請求項５あるいは６に記載のデジタルカメラにおいて、前記シーケンス番号と前記画像データとを組み合わせた画像情報から内部で計算したメッセージダイジェストを、前記収容した秘密鍵を用いて内部で暗号化し、前記画像情報とともに記憶媒体に記録することを特徴とするデジタルカメラ。

【請求項８】　請求項５乃至７のいずれかに記載のデジタルカメラにおいて、少なくとも一の外部認証鍵を収容し、該外部認証鍵に対する外部認証が成立することにより、前記収容したシーケンス番号のリセットが可能であることを特徴とするデジタルカメラ。

【請求項９】　請求項１乃至８のいずれかに記載のデジタルカメラにおいて、画像データを撮影した時刻と該画像データとを組み合わせた画像情報から内部で計算したメッセージダイジェストを、前記収容した秘密鍵を用いて内部で暗号化し、前記画像情報とともに記憶媒体に記録することを特徴とするデジタルカメラ。

【請求項１０】　請求項９に記載のデジタルカメラにおいて、内部で管理している時刻の設定が、外部からの変更禁止属性を有することを特徴とするデジタルカメラ。

2

【請求項１１】　請求項９あるいは１０に記載のデジタルカメラにおいて、少なくとも一の外部認証鍵を収容し、該外部認証鍵が成立することにより、内部で管理している時刻の設定変更が可能であることを特徴とするデジタルカメラ。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、デジタルカメラ、より詳細には、デジタルカメラで撮影した画像データのセキュリティに関し、一般的なデータセキュリティに応用可能なセキュリティシステムに関する。

【０００２】

【従来の技術】デジタルカメラで証拠画像を撮影する技術としては、例えば、特開平７－５０８２７号公報「ディジタル電子カメラを用いた事故監視システム」が挙げられる。これは、自動車に搭載するデジタルカメラを用いた事故監視システムに関するもので、撮影した画像データに対して、事故関連状況の画像関連情報を正確に記録し、さらに、証拠穏滅やデータの書き換えを禁止することにより、画像データの証拠性を高めるというものである。その請求項２において、「一定条件の暗号設定方法で消去や書き込みを可能とすることを特徴とする」という記載があり、その部分が画像データの証拠隠滅や改ざんを防ぐ核となる技術になる。

【０００３】

【発明が解決しようとする課題】しかしながら、上記特開平７－５０８２７号公報の実施例には、上記暗号設定についての具体的な技術や方法の開示がなく、実施可能となっていない。また、従来、通常のフィルムを使用して撮影された写真は、フィルム内のコマが時系列的に並んでおり、撮影した順序が明確になっていることから、現像したフィルムを参照すれば、撮影された事実の順序関係がわかり、その上、そのフィルムを偽造して、撮影された順序を入れ替えたり、画像を改変することは非常に困難である。しかし、デジタルカメラで撮影された画像データは、データそのものがデジタルであるため、改ざんや消去，データの入れ替えなどを、何の痕跡も残さずに実行することが容易であり、従来のフィルムベースのカメラで撮影されたものに比べ、撮影された画像、すなわち、事実の証明力が低くなっているのが現状である。

【０００４】本発明は、上述のような実情を考慮してなされたもので、撮影した画像データの証明力を高めたデジタルカメラを提供することを目的としてなされたものである。

【０００５】

【課題を解決するための手段】請求項１の発明は、公開鍵暗号方式の認証に用いる少なくとも一対の公開鍵及び秘密鍵を、公開鍵と該公開鍵に対する公証機関のデジタル署名とからなる公開鍵証明書及び秘密鍵として収容

し、公開鍵暗号方式の暗号アルゴリズムとメッセージダイジェストの生成アルゴリズムとを搭載したことを特徴とし、デジタルカメラ単体で、画像データに署名を付加するようにしたものである。

【０００６】請求項２の発明は、請求項１の発明において、前記収容した秘密鍵が、外部読出禁止属性を有し、撮影した画像データから内部で計算したメッセージダイジェストを、前記秘密鍵を用いて内部で暗号化し、前記画像データとともに記憶媒体に記録することを特徴とし、署名のセキュリティを高めるようにしたものである。

【０００７】請求項３の発明は、請求項１あるいは２の発明において、前記収容した公開鍵証明書が、外部からの書換禁止属性を有することを特徴とし、画像データに付加された署名の検証が確実に行えるようにしたものである。

【０００８】請求項４の発明は、請求項１乃至３の発明のいずれかの発明において、少なくとも一の外部認証鍵を収容し、該外部認証鍵に対する外部認証が成立することにより、前記収容した秘密鍵あるいは公開鍵証明書の書き換えが可能であることを特徴とし、特別な条件を満たした場合にのみ、収容されている秘密鍵や公開鍵証明書を変更できるようにしたものである。

【０００９】請求項５の発明は、請求項１乃至４のいずれかの発明において、撮影した画像の枚数を表わすシーケンス番号を収容し、該シーケンス番号を、撮影した画像データとともに記憶媒体に記録することを特徴とし、画像のシーケンス番号を記録するようにしたものである。

【００１０】請求項６の発明は、請求項５の発明において、前記収容したシーケンス番号が、外部からの書換禁止属性を有することを特徴とし、画像のシーケンス番号を外部から変更できないようにしたものである。

【００１１】請求項７の発明は、請求項５あるいは６の発明において、前記シーケンス番号と前記画像データとを組み合わせた画像情報から内部で計算したメッセージダイジェストを、前記収容した秘密鍵を用いて内部で暗号化し、前記画像情報とともに記憶媒体に記録することを特徴とし、シーケンス番号と画像データとを切り離せないようにしたものである。

【００１２】請求項８の発明は、請求項５乃至７のいずれかの発明において、少なくとも一の外部認証鍵を収容し、該外部認証鍵に対する外部認証が成立することにより、前記収容したシーケンス番号のリセットが可能であることを特徴とし、特別な条件を満たした場合にのみ、収容されているシーケンス番号をリセットできるようにしたものある。

【００１３】請求項９の発明は、請求項１乃至８のいずれかの発明において、画像データを撮影した時刻と該画像データとを組み合わせた画像情報から内部で計算した

メッセージダイジェストを、前記収容した秘密鍵を用いて内部で暗号化し、前記画像情報とともに記憶媒体に記録することを特徴とし、内部で管理している時刻の設定を画像データとともに切り離せない状態で記録するようにしたものである。

【００１４】請求項１０の発明は、請求項９の発明において、内部で管理している時刻の設定が、外部からの変更禁止属性を有することを特徴とし、内部で管理している時刻の設定を外部から変更できないようにしたものである。

【００１５】請求項１１の発明は、請求項９あるいは１０の発明において、少なくとも一の外部認証鍵を収容し、該外部認証鍵が成立することにより、内部で管理している時刻の設定変更が可能であることを特徴とし、特別な条件を満たした場合にのみ、内部で管理している時刻の設定を変更できるようにしたものである。

【００１６】

【発明の実施の形態】図１は、本発明によるデジタルカメラの一実施例を説明するための構成図で、図中、１はＣＣＤ、２はＲＯＭ、３はＲＡＭ、４はＣＰＵ、５はＥＥＰＲＯＭ、６は通信ポート、７はタイマ、８は外部メモリで、ＲＯＭ２には、標準的な暗号アルゴリズム（例えば、米国特許４４０５８２９号に示されるＲＳＡやＤＥＳ(Data Encryption Standard)。ＤＥＳは外部認証に使用する可能性がある。），メッセージダイジェスト生成アルゴリズム（例えば、ＭＤ５），画像データ圧縮アルゴリズム（例えば、ＪＰＥＧ）、乱数発生アルゴリズム，メイン制御プログラムが格納される。ＥＥＰＲＯＭ５には、公開鍵暗号方式の秘密鍵と、公開鍵証明書（公証機関の署名と公開鍵），シーケンス番号，外部認証鍵が格納される。ＲＡＭ３には、メイン制御プログラム，各種アルゴリズム，秘密鍵，シーケンス番号，外部認証鍵等が必要に応じてロードされる。外部メモリ（例えば、メモリカード等）８には、撮影した画像データに、シーケンス番号，時刻，署名などを付加した画像情報を記録する。なお、ここで、アルゴリズムはプログラムを意味する。

【００１７】シャッターボタンが押されると、ＣＰＵ４はタイマから時刻を取得し、それをＲＡＭ３に記憶すると同時に、ＣＣＤ１から撮影画像データを取得し、ＲＡＭ３に収容する。そして、収容した画像データを圧縮する。ＥＥＰＲＯＭ５からシーケンス番号を取り出すと同時に、シーケンス番号に１加えたシーケンス番号をＥＥＰＲＯＭ５に記録する。次に、圧縮した画像データの先頭に先に取り出したシーケンス番号と、タイマから取得した時刻データとを付加する。そして、できあがった画像情報に対してメッセージダイジェストアルゴリズム（例えば、ＭＤ５）を使用したメッセージダイジェストを計算する。ＥＥＰＲＯＭ５から秘密鍵を読み出し、それを使用して先に計算したメッセージダイジェストを暗

5

号化する。そして、得られた署名を先の画像情報の最後に付加して一塊の撮影情報とし、外部メモリ８に記録する。

【００１８】秘密鍵，公開鍵証明書，シーケンス番号，時刻設定を変更する際に、あらかじめ行うべき外部認証処理は、以下の手順で行う。外部認証に使用するアルゴリズムがＤＥＳの場合、まず、内部で乱数を発生させ、その乱数を外部装置に送出する。外部装置から認証コードを受け取り、先に生成した乱数を外部認証鍵により暗号化したコードと比較する。それらのコードが一致すれば外部認証が成立したこととし、セキュリティステータス（ＲＡＭで管理しているフラグ。初期状態はＦＡＬＳＥとする。）をＴＲＵＥに変更する。

【００１９】外部から秘密鍵，公開鍵証明書，シーケンス番号，時刻設定の変更を要求された場合には、まず、内部で管理しているセキュリティステータスを参照し、それがＦＡＬＳＥとなっている場合には要求を受け付けない。ＴＲＵＥとなっている場合には要求を受けつけ、その要求に応じた処理を行う。処理を行うとセキュリティステータスをＦＡＬＳＥに変更する。

【００２０】

【発明の効果】請求項１の発明は、公開鍵暗号方式の認証に用いる少なくとも一対の公開鍵及び秘密鍵を、公開鍵と該公開鍵に対する公証機関のデジタル署名とからなる公開鍵証明書及び秘密鍵として収容し、公開鍵暗号方式の暗号アルゴリズムとメッセージダイジェストの生成アルゴリズムとを搭載したので、撮影した画像に署名を付加する際に必要な情報、および、アルゴリズムにより、デジタルカメラ単体で画像データに署名を付加することができ、撮影した画像データの証明力を高めることができる。

【００２１】請求項２の発明は、請求項１の発明において、前記収容した秘密鍵が、外部読出禁止属性を有し、撮影した画像データから内部で計算したメッセージダイジェストを、前記秘密鍵を用いて内部で暗号化し、前記画像データとともに記憶媒体に記録するので、署名の生成に使用する秘密鍵の外部からの参照が不可能となり、これにより、署名のセキュリティを高めることができ、撮影した画像に署名（メッセージダイジェストを暗号化したもの）を撮影した画像データに署名（メッセージダイジェストを暗号化したもの）を付加することによって、画像データを撮影したデジタルカメラを特定し、撮影された画像データの証明力を高めることができる。

【００２２】請求項３の発明は、請求項１あるいは２の発明において、前記収容した公開鍵証明書が、外部からの書換禁止属性を有するので、公開鍵証明書の外部からの書き換えが不可能となり、これにより、デジタルカメラによって画像データに付加された署名の検証が確実に行え、画像データを撮影したデジタルカメラを特定し、撮影された画像データの証明力を高めることができる。

6

【００２３】請求項４の発明は、請求項１乃至３のいずれかの発明において、少なくとも一の外部認証鍵を収容し、該外部認証鍵に対する外部認証が成立することにより、前記収容した秘密鍵あるいは公開鍵証明書の書き換えが可能であるので、特別な条件を満たした場合にのみ、収容されている秘密鍵や公開鍵証明書の変更が可能となり、これにより、秘密鍵や公開鍵証明書のセキュリティを保つことでき、さらに、定期的な鍵の更新が可能になって、秘密鍵のセキュリティが高まり、撮影した画像の証明力を高めることができる。

【００２４】請求項５の発明は、請求項１乃至４のいずれかの発明において、撮影した画像の枚数を表わすシーケンス番号を収容し、該シーケンス番号を、撮影した画像データとともに記憶媒体に記録するので、画像のシーケンス番号の記録により、フィルムベースのカメラで実現されていた事実の前後関係に関する証明力を高めることができる。

【００２５】請求項６の発明は、請求項５の発明において、前記収容したシーケンス番号が、外部からの書換禁止属性を有するので、画像のシーケンス番号の外部からの変更が不可能となり、これにより、シーケンス番号のセキュリティを高めることができ、事実の前後関係に関する証明力を高めることができる。

【００２６】請求項７の発明は、請求項５あるいは６の発明において、前記シーケンス番号と前記画像データとを組み合わせた画像情報から内部で計算したメッセージダイジェストを、前記収容した秘密鍵を用いて内部で暗号化し、前記画像情報とともに記憶媒体に記録するので、シーケンス番号と画像データとを合わせてメッセージダイジェストを計算して署名を作成し、これにより、シーケンス番号と画像データとを切り離せないものにすることができ、そのシーケンス番号により事実の前後関係に関する証明力を高めることができる。

【００２７】請求項８の発明は、請求項５乃至７のいずれかの発明において、少なくとも一の外部認証鍵を収容し、該外部認証鍵に対する外部認証が成立することにより、前記収容したシーケンス番号のリセットが可能であるので、特別な条件を満たした場合にのみ、収容されているシーケンス番号をリセット可能とすることによって、シーケンス番号のセキュリティを保つことができ、さらに、定期的にシーケンス番号をリセットすることによって、事実の前後関係を証明するに役立つ範囲でシーケンス番号を管理することができ、むやみにシーケンス番号が大きくなり、扱いにくい番号になることを防ぐことができる。

【００２８】請求項９の発明は、請求項１乃至８のいずれかの発明において、画像データを撮影した時刻と該画像データとを組み合わせた画像情報から内部で計算したメッセージダイジェストを、前記収容した秘密鍵を用いて内部で暗号化し、前記画像情報とともに記憶媒体に記

7

録するので、内部で管理している時刻を画像データとともに切り離せない状態で記録し、これにより、画像データが撮影された時刻に関する証明力を高めることができる。

【００２９】請求項１０の発明は、請求項９の発明において、内部で管理している時刻の設定が、外部からの変更禁止属性を有するので、内部で管理している時刻設定の外部からの変更を可能とし、これにより、時刻の設定に関するセキュリティを高めることができ、画像データが撮影された時刻に関する証明力を高めることができる。

【００３０】請求項１１の発明は、請求項９あるいは１０の発明において、少なくとも一の外部認証鍵を収容し、該外部認証暗が成立することにより、内部で管理している時刻の設定変更が可能であるので、特別な条件を満たした場合にのみ、内部で管理している時刻設定の変更を可能とし、これにより、時刻の設定に関するセキュリティを保ちつつ、定期的に正確な時刻に設定することができ、画像データが撮影された時刻に関する証明力を高めることができる。

8

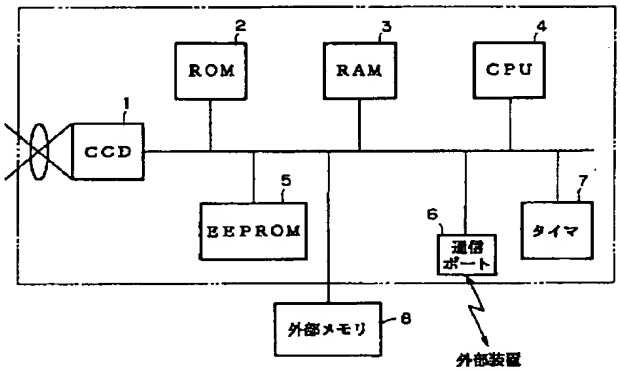
【図面の簡単な説明】

【図１】　本発明によるデジタルカメラの一実施例を説明するための構成図である。

【符号の説明】

１…ＣＣＤ、２…ＲＯＭ、３…ＲＡＭ、４…ＣＰＵ、５…ＥＥＰＲＯＭ、６…通信ポート、７…タイマ、８…外部メモリ。

【図１】



フロントページの続き

(51) Int. Cl. 6		識別記号	FI		
Ｈ０４Ｎ	5/225		Ｈ０４Ｌ	9/00	６７５Ｄ
	5/232		Ｈ０４Ｎ	5/91	Ｋ
	5/915				